UNITED STATES PATENT AND TRADEMARK OFFICE

**UNITED STATES DEPARTMENT OF COMMERCE**
**United States Patent and Trademark Office**
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/614,343 | 07/08/2003 | Gabor Bajko | 39700-591001US/NC39808US | 7843 |

64046 7590 02/16/2010

MINTZ, LEVIN, COHN, FERRIS, GLOVSKY AND POPEO, P.C
ONE FINANCIAL CENTER
BOSTON, MA 02111

| EXAMINER | |
|---|---|
| MACILWINEN, JOHN MOORE JAIN | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2442 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 02/16/2010 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| | | | |
|---|---|---|---|
| ***Office Action Summary*** | **Application No.**<br>10/614,343 | **Applicant(s)**<br>BAJKO, GABOR | |
| | **Examiner**<br>John M. MacIlwinen | **Art Unit**<br>2442 | |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *12 November 2009*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1,2,4-10,13,22-25,46 and 56-71* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-10,13,22-25,46 and 56-71* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

## DETAILED ACTION

### *Response to Arguments*

1. Applicant's arguments filed 11/12/2009 have been fully considered.

2. Applicant argues on pages 10 – 12, said arguments directed on page 11 to if Marshall teaches "whether a verification check that a proxy performed has been successful" instead of teaching "an indication of whether the message has been through a security check at the first layer prior to being received at the proxy". Applicant argues on page 10 that in [55] of their specification they show using the tag "screening=no" to indicate said indication.

Jennings provides teachings regarding said apparatus performing forwarding as well as said determining (represented by Jennings "proxy" in Section 5).

Marshalls' "rpi-screen = no" (page 20, paragraph 5) corresponds to Applicant's "screening = no" (Applicant's specification, [55], Applicant's arguments, pg. 10).

In the teachings of Jennings in view of Marshall and 3GPP, the "rpi-screen=yes or not" can be used as the claimed second layer indication (as said "rpi-screen" is a SIP parameter, SIP being an Application layer protocol).

Jennings in view of Marshall and 3GPP teach where a SEG-A receives a message from a SEG-B (3GPP, Fig. 1). When said message comes via the Za interface, then SEG-A adds an "rpi-screen=yes" parameter prior to forwarding the message to the next hop within the first network (Marshall, pg. 20, paragraph 6), said message, received from the "trusted entity" SEG-B (Marshall, pg. 20, paragraph 1). Since said message is from the trusted entity SEG-B, said message would have also been through a security check (shown through 3GPP's teachings that SEG-B and SEG-A are communicating "in direct communication …. [and] maintain[ing] secured … tunnels" and thus communication between them is "afforded … security protection" (3GPP, 5.3.1, pg. 1) due to the "negotiate[ed] … secure tunnel between them" (3GPP, 5.3.2)).

Else if the message was not from a trusted entity (one over an interface over Za) and thus had not been through a security check, "rpi-screen=no" parameter prior would be added to prior forwarding (Marshall, page 20 paragraphs 3 and 5).

Za uses IP-Sec security, which is at the Network Layer, a layer lower than the Application Layer (of SIP) and thus the SIP security indication meets the claim limitation of being at "higher layer than the first layer".

Based on the clarifications provided by Applicant's claim amendments, the explanations and mapping accompanying in the pending rejection has been further clarified.

### *Claim Rejections - 35 USC § 101*

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 1, 2, 4 – 10, 13, 22 – 24, 46, 63 – 68 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

5. Regarding claims 1, 2, 4 – 10, 13, and 63 – 67, said claims are directed to an apparatus comprising a determiner, forwarder, modifier, etc. configured to…

Paragraph 37 of Applicant's specification, for example, states that "...components are all provided with suitable software for performing various functions and can be set up ... by suitable programming. Some functions may be hardware based".

Thus based on Applicant's specification, it appears that said the items "configured to" perform various functionality could be embodied solely by software.

6. Regarding claims 22 – 24 and 68, said claims are directed to "a security server" and a "network processing element" configured to perform various functionality/processes.

Based on Applicant's specification, it appears that said "security server" and "network processing element" may correspond to the "components" cited above in paragraph 37, said components corresponding solely to software. Thus it appears that said claims may be directed solely to software.

7. Regarding claim 46, said claim is directed to "an apparatus" comprising "means for".

Based on Applicant's specification, it appears that said "apparatus" and various "means for" may correspond to the "components", cited above in paragraph 37, said components corresponding solely to software.

Thus it appears that said claim 46 may be directed solely to software.

### *Claim Rejections - 35 USC § 103*

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and

> the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1, 2, 4-10, 22-25, 46 and 56-71 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jennings and Peterson (RFC 3325 Internet Draft, http://tools.ietf.org/html/draft-ietf-sip-asserted-identity-00, May 27, 2002), hereafter Jennings, in view of W. Marshall et al. (draft-ietf-sip-privacy-04.txt, February 27, 2002), hereafter Marshall, further in view of 3GPP TSG SA WG3 Security – S3#18, Proposed changes to 33.2000 about Za, Zb, Zc interfaces, hereafter 3GPP.

10. Regarding claim 1, Jennings shows an apparatus comprising a determiner configured to determine whether a message received at a first network has been through a security check by determining whether or not the message has been received with security (i.e., from a node that is in its “trust domain”, see section 5)

a forwarder configured to forward the message within the first network regardless of the result of the determination (section 4)

and utilizing security indications on the Application layer (via showing represented by showing P-Asserted-Identity and thus security indications in the SIP header, SIP being an Application layer protocol and thus being in the top-most network layer).

Jennings additionally shows selectively performing message modifications. Jennings does not, however, explicitly show all of:

determining whether or not a message has been received with security at a first layer;

a modifier configured to modify the message so as to indicate a second layer indication that the message has not been though a security check at the first layer prior to being received at the first network when the result of the determination is that the message has not been through a security check, wherein the second layer is a higher layer than the first layer.

Marshall determining whether or not a message has been received with security (via checking if the message was from a trusted entity via checking if the message includes a security and trust verification parameter, pg. 20 paragraph 6 where in Marshall trusted entities have performed security checks on the messages they send, pg. 11 and pg. 21 paragraph 3,7 );

a modifier configured to modify the message so as to include a second layer indication that the message has not been though a security check at the first layer prior to being received at the first network when the result of the determination is that the message has not been through a security check (pg. 20, paragraph 3 and 5, showing adding an “rpi-screen=no” parameter).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Jennings with that of Marshall because both disclosures are IETF drafts addressing SIP, and are thus designed to complement each other and be used together.

Jennings in view of Marshall do not explicitly show receiving a message with security at a first layer, wherein the second layer is a higher layer than the first layer.

3GPP shows receiving a message with security at a first layer wherein the second layer is a higher layer than the first layer (3GPP, 5.3.1 and 5.3.2, showing receiving messages over a Za interface, which includes IPSec, also known as IP Security, which is a Network Layer protocol and thus at a lower layer than the Application Layer security used by Jennings in view of Marshall).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Jennings in view of Peterson and 3GPP in order to further utilize developing standards, helping to assure compliant and predictable operation.

Jennings in view of Marshall and 3GPP thus show where a proxy/security gateway SEG-A receives a message from a SEG-B (3GPP, Fig. 1). When said message comes via the Za interface, SEG-A adds an “rpi-screen=yes” parameter prior to forwarding the message to the next hop within the first network (Marshall, pg. 20, paragraph 6), said message, received from the “trusted entity” SEG-B (Marshall, pg. 20, paragraph 1). Since said message is from the trusted entity SEG-B, said message would have been through a security check as said messages are sent over the Za interface (shown through 3GPP’s teachings that SEG-B and SEG-A are communicating "in direct communication …. [and] maintain[ing] secured … tunnels” and thus communication between them is “afforded … security protection” (3GPP, 5.3.1, pg. 1) due to the "negotiate[ed] … secure tunnel between them” (3GPP, 5.3.2)).

11. Regarding claim 2, Jennings in view of Marshall and 3GPP further comprising a receiver configured to receive messages via a secure interface and a second network

(3GPP, Fig. 1, Jennings, section 5) and directly from outside the first network (Jennings, sections 5 and 6).

12. Regarding claim 4, Jennings in view of Marshall and 3GPP further show wherein the message comprises a second layer identity header (Jennings, Sections 4 and 5, represented the SIP header which includes P-Asserted-Identity), and wherein the modifier is configured to include the second layer indication in the second layer identity header of the message (Jennings, sections 4 and 5).

13. Regarding claim 5, Jennings in view of Marshall and 3GPP further show wherein the message comprises a session initiation protocol message (Jennings, section 5).

14. Regarding claim 6, Jennings in view of Marshall and 3GPP further show wherein the identity header comprises a p-Asserted-Identity (Jennings, 5 and 12).

15. Regarding claim 7, Jennings in view of Marshall and 3GPP further show wherein the message comprises a second layer identity header, and wherein the modifier is further configured to modify the message so as to indicate that the message has not been through a security check by removing at least part of the second layer identity header (Marshall, 6.1 and 7.5).

16. Regarding claim 8, Jennings in view of Marshall and 3GPP further show a detector configured to detect whether the second layer identity header is of a particular type and when so to remove at least part of the header (Jennings, 4 and 7).

17. Regarding claim 9, Jennings in view of Marshall and 3GPP further show wherein the message comprises a session initiation protocol message (Jennings, 7).

18. Regarding claim 10, Jennings in view of Marshall and 3GPP further show wherein the detector is configured to detect whether the second layer identity header comprises a p-Asserted-Identity type (Jennings, 7).

19. Regarding claim 22, Jennings shows a security server ("proxy", section 5); and

a network processing element ("node", section 5) the security server being configured to receive a message, perform a security determination and forward the message to the network processing element regardless of the result of the determination (Sections 4 and 5).

Jennings does not explicitly show all of: determine whether a message has been through a security check be determining whether or not the message has been receiving with security at a first layer, when the result of the determination is that the message has not been though a security check at the first layer prior to being received at the security server, wherein the second layer is higher than the first layer, and forward the message to the network processing element regardless of the result of the determination.

Marshall determining whether or not a message has been received with security (via checking if the message was from a trusted entity via checking if the message includes a security and trust verification parameter, pg. 20 paragraph 6 where in Marshall trusted entities have performed security checks on the messages they send, pg. 11 and pg. 21 paragraph 3,7);

when the result of the determination is that the message has not been through a security check modify the message so as to include a second layer indication that the message has not been though a security check at the first layer prior to being received at the security server (pg. 20, paragraph 3 and 5, showing adding an “rpi-screen=no” parameter).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Jennings with that of Marshall because both disclosures are IETF drafts addressing SIP, and are thus designed to complement each other and be used together.

Jennings in view of Marshall do not explicitly show receiving a message with security at a first layer, wherein the second layer is a higher layer than the first layer.

3GPP shows receiving a message with security at a first layer wherein the second layer is a higher layer than the first layer (3GPP, 5.3.1 and 5.3.2, showing receiving messages over a Za interface, which includes IPSec, also known as IP Security, which is a Network Layer protocol and thus at a lower layer than the Application Layer security used by Jennings in view of Marshall).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Jennings in view of Peterson and 3GPP in order to further utilize developing standards, helping to assure compliant and predictable operation.

20. Regarding claim 23, Jennings in view of Marshall and 3GPP further show wherein the security server is configured to receive messages via a secure interface (3GPP, pg. 2) and another security domain and directly from outside the system (Jennings, sections 5 and 6).

21. Regarding claim 24, Jennings in view of Marshall and 3GPP further show wherein the network processing element is configured to receive a message forwarded by the security server and determine whether the message has been modified so as to include a second layer indication that the message has not been through a security check, and when the message has been so modified, perform one or more security checks in respect of the message (Jennings, section 5 and Marshall, 6.1 and 7.5)

22. Regarding claim 25, Jennings shows a method comprising determining whether a message received at a first network has not been through a security check by determining whether or not the message has been received with security (i.e., from a node that is in its "trust domain", see section 5)

utilizing security indications on the Application layer (via showing represented by showing P-Asserted-Identity and thus security indications in the SIP header, SIP being an Application layer protocol and thus being in the top-most network layer) and

forwarding the message within the first network (section 4)

Jennings additionally shows selectively performing message modifications. Jennings does not, however, explicitly show all of:

determining that a message has been received with security at a first layer;

modifying the message so as to indicate a second layer indication that the message has not been though a security check at the first layer prior to being received at the first network, wherein the second layer is a higher layer than the first layer.

Marshall determining whether or not a message has been received with security (via checking if the message was from a trusted entity via checking if the message includes a security and trust verification parameter, pg. 20 paragraph 6 where in Marshall trusted entities have performed security checks on the messages they send, pg. 11 and pg. 21 paragraph 3,7 );

a modifier configured to modify the message so as to include a second layer indication that the message has not been though a security check at the first layer prior to being received at the first network when the result of the determination is that the message has not been through a security check (pg. 20, paragraph 3 and 5, showing adding an “rpi-screen=no” parameter).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Jennings with that of Marshall because both disclosures are IETF drafts addressing SIP, and are thus designed to complement each other and be used together.

Jennings in view of Marshall do not explicitly show receiving a message with security at a first layer, wherein the second layer is a higher layer than the first layer.

3GPP shows receiving a message with security at a first layer wherein the second layer is a higher layer than the first layer (3GPP, 5.3.1 and 5.3.2, showing receiving messages over a Za interface, which includes IPSec, also known as IP Security, which is a Network Layer protocol and thus at a lower layer than the Application Layer security used by Jennings in view of Marshall).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Jennings in view of Peterson and 3GPP in order to further utilize developing standards, helping to assure compliant and predictable operation.

23. Regarding claim 1, Jennings shows an apparatus comprising determining means for determining whether a message received at a first network has been through a security check by determining whether or not the message has been received with security (i.e., from a node that is in its “trust domain”, see section 5)

and forwarding means for forwarding the message within the first network regardless of the result of the determination (section 4)

and utilizing security indications on the Application layer (via showing represented by showing P-Asserted-Identity and thus security indications in the SIP header, SIP being an Application layer protocol and thus being in the top-most network layer).

Jennings additionally shows selectively performing message modifications. Jennings does not, however, explicitly show all of:

determining whether a message has been received with security at a first layer;

and modifying means for, when the message is determined not to have been through a security check, modifying the message to include a second layer indication that the message has not been though a security check at the first layer prior to being received at the first network, wherein the second layer is a higher layer than the first layer.

Marshall determining whether a message has been received with security (via checking if the message was from a trusted entity via checking if the message includes a security and trust verification parameter, pg. 20 paragraph 6 where in Marshall trusted entities have performed security checks on the messages they send, pg. 11 and pg. 21 paragraph 3,7 );

and modifying means for, when the message is determined not to have been through a security check, modifying the message to include a second layer indication that the message has not been though a security check at the first layer prior to being received at the first network (pg. 20, paragraph 3 and 5, showing adding an “rpi-screen=no” parameter).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Jennings with that of Marshall because both disclosures are IETF drafts addressing SIP, and are thus designed to complement each other and be used together.

Jennings in view of Marshall do not explicitly show receiving a message with security at a first layer, wherein the second layer is a higher layer than the first layer.

3GPP shows receiving a message with security at a first layer wherein the second layer is a higher layer than the first layer (3GPP, 5.3.1 and 5.3.2, showing receiving messages over a Za interface, which includes IPSec, also known as IP Security, which is a Network Layer protocol and thus at a lower layer than the Application Layer security used by Jennings in view of Marshall).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Jennings in view of Peterson and 3GPP in order to further utilize developing standards, helping to assure compliant and predictable operation.

24. Regarding claim 56, Jennings in view of Marshall and 3GPP further show wherein the message comprises a second layer identity header, and comprising including the second layer indication in the second layer identity header of the message (Jennings, Sections 4, 5 and 12).

25. Regarding claim 57, Jennings in view of Marshall and 3GPP further show wherein the message comprises a session initiation protocol message (Jennings, Sections 4, 5 and 12).

26. Regarding claim 58, Jennings in view of Marshall and 3GPP further show wherein the identity header comprises a p-Asserted-Identity (Jennings, Sections 4 and 12).

27. Regarding claim 59, Jennings in view of Marshall and 3GPP further show wherein the message comprises a second layer identity header, and further comprising modifying the message so as to include a second layer indication that the message has not been through a security check by removing at least part of the second layer identity header (Jennings, 4 and 12 and Marshall, 6.1 and 7.5).

28. Regarding claim 60, Jennings in view of Marshall and 3GPP further show detecting whether the second layer identity header is of a particular type and when so removing at least part of the header (Jennings, 4 and 7).

29. Regarding claim 61, Jennings in view of Marshall and 3GPP further show wherein the message comprises a session initiation protocol message (Jennings, 4 and 12).

30. Regarding claim 62, Jennings in view of Marshall and 3GPP further comprising detecting whether the second layer identity header comprises a p-asserted identity type (Jennings, Sections 4 and 12).

31. Regarding claim 63, Jennings in view of Marshall and 3GPP further show wherein the security at a first layer is security applied to a message at a security interface between two security domains (3GPP, Fig. 2, pg. 2).

32. Regarding claim 64, Jennings in view of Marshall and 3GPP further show wherein the security interface is a Za interface (3GPP, Fig. 2, pg. 2).

33. Regarding claim 65, Jennings in view of Marshall and 3GPP further show wherein the forwarder is configured to forward the message over a Zb interface (3GPP, Fig. 2, pg. 2).

34. Regarding claim 66, Jennings in view of Marshall and 3GPP further show wherein the security at a first layer is security applied to a message at a security interface between two security domains (3GPP, Fig. 2, pg. 2).

35. Regarding claim 67, Jennings in view of Marshall and 3GPP further show where the secure interface is a Za interface (3GPP, Fig. 2, pg. 2).

36. Regarding claim 68, Jennings in view of Marshall and 3GPP further show wherein the security server is configured to forward the message to the network processing element over a Zb interface (3GPP, Fig. 2, pg. 2).

37. Regarding claim 69, Jennings in view of Marshall and 3GPP further show wherein the security at a first layer is a security applied to a message at a secure interface between two security domains (3GPP, Fig. 2, pg. 2).

38. Regarding claim 70, Jennings in view of Marshall and 3GPP further show wherein the security interface is a Za interface (3GPP, Fig. 2, pg. 2).

39. Regarding claim 71, Jennings in view of Marshall and 3GPP further show comprising forwarding the message within the first network over a Zb interface (3GPP, Fig. 2, pg. 2).

40. Claim 13 rejected under 35 U.S.C. 103(a) as being unpatentable over Jennings in view of Marshall as applied to claim1 above, and further in view of Soininen (RFC 3574 Internet Draft, http://tools.ietf.org/html/draft-ietf-v6ops-3gpp-cases-00, September, 2002).

Jennings and in view of Marshall and 3GPP show claim 1.

Jennings and in view of Marshall and 3GPP do not show an interrogating call session control function.

Soininen shows where an apparatus comprises and utilized an interrogating call session control function (Section 3.2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Jennings and in view of Marshall and 3GPP with that of Soininen in order to provide for an SIP system adhering to the 3GPP networking standard (Soininen, Section 3.2).

## *Conclusion*

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John M. MacIlwinen whose telephone number is (571) 272-9686. The examiner can normally be reached on M-F 7:30AM - 5:00PM EST; off alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joon Hwang, can be reached on (571) 272 - 4036. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

John MacIlwinen

(571) 213 – 6095

/Joon H. Hwang/
Supervisory Patent Examiner, Art Unit 2447